

Gestion des appareils mobiles: un mystère pour 39% des PME françaises

Accessoire

Posté par : JPilo

Publié le : 7/12/2012 14:00:00

Une étude d'Absolute Software révèle que la gestion du phénomène du BYOD et la sécurité des données sur appareils mobiles ne sont toujours pas une priorité pour de nombreuses entreprises.

Absolute Software Corporation, spécialiste des logiciels et services de gestion et de sécurisation des ordinateurs et des appareils mobiles (PC, Mac, iOS, Android et Blackberry), publie les résultats d'une nouvelle recherche indiquant que près de 40% des entreprises françaises n'ont pas mis en place de politique ni même de règles pour gérer l'utilisation des appareils mobiles sur le lieu de travail.

Le cabinet indépendant Vanson Bourne, spécialiste des études sur le marché des technologies, a mené l'enquête pour le compte du fournisseur de solutions de sécurité directement intégrées au micro logiciel et de gestion des terminaux mobiles. Le projet a porté sur 1 200 décideurs informatiques de différents secteurs verticaux, à travers le Royaume-Uni, la France, l'Allemagne et les États-Unis. L'étude met en lumière les principales tendances dans la gestion des appareils mobiles, leur sécurisation et ceux privilégiés sur le lieu de travail.

The logo for Absolute Software, with 'Absolute' in a bold blue font and 'Software' in a brown font, with a registered trademark symbol.

« Les services informatiques examinent le spectre de la mobilité ainsi que tous les problèmes de sécurité qu'elle comporte depuis deux ans déjà. Il est particulièrement inquiétant de constater que beaucoup d'entreprises ne prennent pas de mesures pour sécuriser et gérer correctement leurs appareils mobiles. Compte tenu de l'ampleur des risques financiers et commerciaux qui peut engendrer la perte de données, il est surprenant de remarquer que les entreprises ne font toujours pas de la sécurité leur priorité », déclare **John Livingston**, Président et Directeur Général d'Absolute Software. « De nouveaux appareils font leur entrée au sein des entreprises et les employés ont de nouvelles attentes en termes d'accès aux applications professionnelles et à leurs données sur le terrain. Les équipes informatiques font alors face à un défi de plus en plus grand et doivent organiser des déploiements sur toute sorte de modèles d'appareils fonctionnant avec des systèmes d'exploitation différents »

BYOD versus informatique

Concernant la fourniture des appareils mobiles, 15% des sociétés françaises comptent sur leurs employés pour apporter leur propre appareil (BYOD), ce qui crée un environnement

extrêmement diversifié que le service informatique doit gérer et sécuriser. Aux États-Unis, près d'une entreprise sur cinq (18%) autorise l'utilisation d'appareils mobiles personnels à des fins professionnelles sur le lieu du travail. En Allemagne, 16% autorisent leur utilisation alors que seulement 7% des entreprises britanniques permettent aux employés d'utiliser leurs appareils personnels.

Au Royaume-Uni, la majorité des organisations (38%) propose un modèle hybride, permettant aux employés d'utiliser leurs propres appareils tout en leur fournissant des appareils de la marque de leur choix appartenant à la société. Aux États-Unis, la majorité (42%) des entreprises interrogées a également adopté cette tactique. La France et l'Allemagne préfèrent mettre en place « COPE » (Corporate Owned Personally Enabled). Elle permet aux employés de choisir un appareil mobile qui serait acheté, possédé et géré par l'entreprise, mais utilisé à la fois à des fins personnelles et professionnelles.

Le Royaume-Uni, la France et l'Allemagne sont les pays les plus restrictifs lorsqu'il est question de gestion des appareils mobiles puisque 3 entreprises sur 10 déclarent qu'elles ne permettent ni le choix d'appareil ni l'utilisation des dispositifs personnels et que seul le service informatique décide quels périphériques et plateformes les employés peuvent utiliser. Aux États-Unis, 15% seulement des entreprises adoptent cette approche stricte, conduite par les départements informatiques.

Sécurisation des données de l'entreprise

La sécurisation des données de l'entreprise sur les appareils mobiles est une préoccupation majeure pour nombre d'entre elles. La méthode la plus commune de sécurisation de ces données sur un smartphone ou une tablette est l'accord donné par les employés pour que le service informatique effectue un verrouillage à distance et efface le contenu de l'appareil lorsqu'il est perdu ou volé. C'est le cas pour deux tiers (65%) des entreprises françaises. Cependant, 11% de ces dernières ont indiqué n'avoir rien mis en place pour sécuriser les données sur les appareils mobiles. À l'inverse, les États-Unis sont plus actifs en matière de sécurité avec seulement 8% des entreprises interrogées rapportant qu'elles ne prennent aucune mesure pour sécuriser les données sur les appareils mobiles.

Lorsqu'il s'agit de restreindre l'accès, environ la moitié des entreprises françaises (51%) utilisent une solution d'accès sécurisé au réseau (NAC) ou une passerelle et 26% autorisent l'accès via un outil gestion des appareils mobiles (MDM). Elles assurent ainsi de l'intégrité de l'appareil puisque l'accès se fait selon les clauses NAC basées sur un profil des appareils à risque et ses utilisateurs. Près d'un tiers des entreprises françaises (24%) permettent tous l'accès aux appareils mobiles via un mot de passe et 6% ne limitent pas l'accès à tous.

« La croissance du marché des technologies grand public a laissé derrière elle l'entreprise qui peine à fournir des appareils de pointe à ses employés. Sur de nombreux lieux de travail, les employés doivent utiliser des appareils moins récents et plus lents que le leur et nombre d'entre eux tentent de contourner le problème en accédant à des données professionnelles via leurs appareils personnels, non sécurisés. Les transferts de données entre plusieurs périphériques indépendants conduit inévitablement à des problèmes de sécurité », déclare **John Livingston**.

« Alors que de nombreuses entreprises cherchent à satisfaire leurs employés en leur permettant de choisir leurs appareils ou utiliser les leurs, un grand nombre a encore du mal à concilier la sécurité avec la plus grande liberté et mobilité exigées par les employés. En dépit de la croissance et de la résonance des phénomènes de la mobilité et du BYOD ces dernières années, aucune décision ne semble prise sur le meilleur mode de gestion de ces tendances. Dans certains cas, les entreprises ont même choisi d'ignorer le problème lorsqu'elles y

sont confrontées. Malgré la maturité des tendances liées à la mobilité, la gestion et la sécurisation des appareils mobiles sur le lieu de travail sont étonnamment immatures. Cette immaturité est une zone de danger pour les entreprises, en particulier au moment où les législateurs de l'UE réfléchissent à une révision des règles autour de la réglementation des données », conclut-il.